AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

CONFRONTING RESURGENT RUSSIA: U.S. AIR FORCE GLOBAL STRIKE CONTRIBUTIONS TO NATIONAL DETERRENT STRATEGY

by

Matthew T. Genelin, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Lt Col Jonathan Arnett

Maxwell Air Force Base, Alabama

April 2010

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government of Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Abstract

As evidenced by their military intervention in South Ossetia, it is clear that Russia is attempting to reestablish their sphere of influence in the surrounding region. Their leadership, especially Prime Minister Putin, also appear steadfast in their efforts to recreate a resurgent Russia as the world player it once was. Future U.S. presidents must carefully consider changes to national security policy to deal with Russian aggression towards their neighbors. The heart of the strategy must be economic, diplomatic, and information efforts backed up with a credible threat of military action. This paper examines how the Air Force can leverage its global strike capability to contribute to that military threat.

The analysis suggests two specific capabilities the Air Force should cultivate to support flexible deterrent options to deter Russia from military intervention against their neighbors. Specifically, these capabilities are global strike via cyber attack, and non-nuclear global strike via intercontinental bombers and low-observable technology. Cyber and non-nuclear attacks have not historically been part of the strategic deterrence framework with regards to the Soviet Union. However, in the post-Cold War international order, Air Force strategists must consider these less destructive means of deterrence and what additional options they present to the president.

1. Introduction

In the years following the collapse of the Soviet Union, all of the former republics have experienced upheaval and uncertainty. In the case of Russia, the largest and most powerful republic, organized crime and unorganized government led to many questions among Western leaders as to the political direction the former superpower would take. With the rise of Vladimir Putin and his consolidation of power first as president and now prime minister, those questions may have been answered. The present Russian leadership appears intent on reestablishing Russia's former sphere of influence with the ultimate goal of regaining their superpower status--at least in the immediate surrounding region.

As Russia's overall goals become clearer, American leaders must carefully reevaluate our new and evolving relationship. The prospect of a nuclear exchange with Russia now seems far less likely than with the Soviet Union throughout the Cold War. However, recent actions by Russia indicate that tension and conflict will likely arise between Russia and the West. After enduring centuries of invasions from numerous enemies, a resurgent Russia is attempting to exert its influence over several former satellites that at one time provided a comfortable buffer against attacks from outsiders. In light of this newfound assertiveness, the United States must consider what deterrent strategy we will pursue vis-à-vis Russia's regional desires. In particular, the Air Force must develop a concept for its role in deterring Russia's regional aggression beyond the *Strategic Triad* of the Cold War. Department of Defense literature and briefings have already introduced a *New Triad* that provides

> "a mix of strategic offensive and defensive capabilities that include: nuclear and non-nuclear strike capabilities; active and passive defenses; and a robust research, development and industrial infrastructure."[1]

The Air Force will have a major role in the new arrangement. Along with conventional expeditionary air power and air mobility, the Air Force also provides unique, prompt global strike capabilities such as nuclear-armed bombers and Intercontinental Ballistic Missiles (ICBMs). The intricacies of nuclear deterrence have already been heavily analyzed for decades. This paper will instead suggest non-nuclear kinetic and cyberspace global strike capabilities the Air Force should develop and maintain in order to provide flexible deterrent options to the President. These Air Force core capabilities are a necessary part of a greater deterrent strategy in case Russia pursues unwarranted military action against its former Soviet neighbors. The analysis in this paper will focus on how the President can threaten use of the two capabilities as part of denial or punishment strategy that best attacks the vulnerabilities of the Russian center of gravity.

It is important to note that successful national strategy to counteract this type of aggression should primarily focus on diplomacy, international information operations and economic actions. However, the president must also have a wide range of military options at his disposal to back up other efforts. The global strike capabilities outlined in this paper are not particularly palatable. They would entail great risk and would be followed by intense consequences. They would hopefully only be employed after a major breakdown in U.S.-Russian relations and would greatly alter the international status quo. Unfortunately, they are a necessary part of the greater strategy and must be developed and maintained by a professional and dominant Air Force.

[1] Deputy Assistant to SECDEF, "US Nuclear Deterrence"

2. Russia's Interests & Intents

To best predict possible future Russian actions, it is beneficial to analyze their most recent foreign dealings. This section draws lessons from the events in Georgia in 2008 as well as some of the public statements made by their national leaders. The logical conclusion is that Russia will not refrain from limited military action in order to exert its will on the other former Soviet states. The section concludes with application of operational design in an analysis of the centers of gravity (COGs) in order to better understand the areas in which Russia is vulnerable to Air Force global strike.

Conflict in Georgia

The conflict between Russia and Georgia over the separatist movement in South Ossetia in 2008 was more complicated than a casual observer might deduce. It was not simply a powerful neighbor coming to the aid of a repressed minority seeking independence from a repressive state government. Rather, it was a calculated series of events carefully managed by former Soviet intelligence agents reminiscent of Cold War proxy revolutions in Third World nations. It also perhaps reveals the true intentions of the largest of the former Soviet republics. When rebels in South Ossetia increased the violence against the Georgian government, the Russian leadership was at first eerily quiet, in stark contrast to their condemnation and military opposition of Georgian operations in previous years--operations often instigated by direct Russian provocation of dissidents within Georgia. In all cases, the Russian government had consistently demonstrated its perceived role as regional leader of the Caucasus.[2]

In the fall of 2008, the Russians appeared to be letting the unrest in South Ossetia run its course. They expressed diplomatic displeasure at the violence, but their peacekeeping forces did nothing, at least initially, to quell the violence. Upon further analysis it becomes more evident

why Russia allowed the violence to escalate. Several analysts have since concluded that the rebel actions were actually instigated by Moscow.[3] Powerful Russian operatives acting inside South Ossetia had bolstered the rebels' strength and leadership in preparation for the revolt. These provocateurs determined that an increase in violence would prompt a swift response from Georgia and thereby justify military intervention from Moscow. Additionally, many separatists had been issued Russian documentation and passports. After increasingly severe Georgian reprisals, Russian leadership could readily explain sending "peacekeepers" as an effort to safeguard their citizens in a hostile nation. However,

> "…the Russian peacekeeping forces were anything but peacekeepers. Rather, they were a conscious instruments of a policy intended to prevent conflict resolution and eventually move these provinces into formal reincorporation into Russia."[4]

If the Russians were truly interested in a peaceful resolution, the peacekeepers they had in the region could have quieted the tribal violence before the Georgian response. Instead they waited until they could label their attack as a security operation for their own citizens. This in turn provided a perfect opportunity to further exert their control over their neighbors.

The response of the European Union was tepid and unspectacular. After nine months of investigation, the Independent International Fact Finding Mission on the Conflict in Georgia (IIFFMCG) concluded that Georgia had triggered the conflict, although Russia had violated international law with their intervention. Their report also stated that Russia had set the conditions for the war and exploited the action for its own purposes. The E.U. commission leveled claims of war crimes on both sides, but noted many atrocities committed against Georgia were by Ossetian irregulars who "could not be adequately controlled by Russian forces."[5]

Overall, the report spread blame amongst all the players, stating that the conflict was the culmination of a long series of events and that no one could be held solely responsible.[6]

Although they agreed that South Ossetia and Abkhazia have no right to secede, the E.U. commission equivocated between both sides' actions, ignoring international norms allowing sovereign states to police their own territory.[7] To that end, the matter has essentially been concluded with the release of the 1,000 page report. No international criminal court or other sanctions have been employed against either side.

Russian Goals

It is likely that Russian leaders—buoyed by their success in the Caucuses and the lack of international response—will continue attempts to expand their sphere of influence in the region. The natural follow-up analysis for U.S. foreign policy strategists regarding the Russia-Georgia conflict is to determine what the national security goals of this "resurgent" Russia are. They appear to boil down to three main aims. Russian leaders have made it clear that the hegemony of the United States is waning. Their leaders envision a multi-polar international security environment with Russia as a global player alongside the European Union and United States, and as such demand global respect.[8] Secondly, Russia's leadership appears to be using old Soviet tactics of feigned respect for self determination to destroy surrounding governments and rally their peoples around Russia.[9] In this manner, they hope to regain the tight control over their region they once enjoyed. Finally, Russia has successfully leveraged its oil and gas reserves to create an asymmetric interdependence with the European Union. The EU is now more dependent on Russia than vice versa. Consequently, Russia plans to leverage this interdependence to further their influence on key Western states.[10] They will continue to use their influence to dissuade these nations from interfering in Russia's relationships with their neighbors.

Where Next?

Given these security strategies, and based on the pattern established with South Ossetia and Abkhazia, Ukraine seems a logical next target for Russian pressure. Along with Georgia, Ukraine has been toying with the possibility of joining the NATO alliance. Understandably, Russia wants to exert its own influence on Ukraine rather than allow the European Union and United States to do so. Putin has gone so far as to threaten "dismemberment" if Ukraine continues its pursuit of joining NATO by annexing the Crimean peninsula.[11] Leaders in Moscow point to the millions of ethnic Russians living in Ukraine (nearly a third of the population) that will be without a voice if they aligned with NATO. This is probably their most credible reason for opposing a Ukrainian alliance with the West. Tension between the two countries has already resulted in Russia using its most aggressive economic tool: petroleum. They have turned off the oil and gas supply several times in the past decade and have threatened to double Ukraine's gas prices at the 2008 Commonwealth of Independent States conference in St. Petersburg.[12]

The course of action followed in South Ossetia could be followed almost exactly in a future confrontation with Ukraine. Russian operatives would foment anger and a separatist attitude among Russians living in Crimea in response to Ukraine's westernization. While publicly denouncing any violence, they will privately encourage an uprising among the separatists and Russian sympathizers. If Ukraine responds militarily, Russia would feel justified to counter that response in an effort to protect their "oppressed" brothers. The possible results of the conflict include a land grab for Russia, an overt statement to other former Soviet states regarding Russia's attitude towards pro-western movement, or a strengthening of Russian resolve to further extend their influence. Any one of these results would be a net loss for the U.S. and E.U. in terms of international power and prestige. Furthermore, this scenario could play out in a

number of former Soviet states. Ukraine simply appears logically to be the next nation to face possible military conflict with Russia.

Center of Gravity Analysis

When determining a course of action to confront a resurgent Russia, national strategic planners must, among other things, determine their centers of gravity. After the COGs are identified at the strategic, operational, and tactical levels of war, critical factor analysis will reveal how the COGs can be defeated. The focus of this paper is on deterrence. As such, the analysis must center on the decision-makers at the highest level of the Russian government—the strategic level.

Since the fall of the Soviet Union, the Russian government has gone through tumult and turmoil. After struggling to embrace a western-style constitutional democracy, the country has devolved back to a nearly unipolar, vertical system with all power concentrated at the Kremlin, specifically with Prime Minister Vladimir Putin. Mr. Putin was successfully installed as the Russian president on the last day of 1999 by his predecessor, Boris Yeltsin.[13] After spending two four-year terms as president consolidating national power, he was forced by term limits to step aside as and take the position of prime minister. Almost all of his *de-facto* power followed with him.[14] It has also emerged that Mr. Putin will likely run for president again in 2012 as allowed by Russian law. Because the presidential term has since been extended to six years, it is possible, even likely, that the U.S. will have to deal with Vladimir Putin as the leader of Russia until 2024.[15] In light of these facts it follows that Mr. Putin personally is the strategic COG for the newly resurgent Russian government.

COG analysis begins by examining critical capabilities. Mr. Putin has demonstrated an amazing ability to rally the Russian people to exert influence in the region. He has made it clear

that the Russian sphere of influence still includes "the near abroad," or former Soviet states.[16] He inspires nationalism among Russians and reminds them of their past glory. Additionally, Russians remember the multiple invasions that they have incurred over the centuries. The population realizes the need for a solid buffer against the outside world and the former satellite states provide just such a barrier. When Mr. Putin orders an incursion into a neighboring country to enforce Russia's vision of the eastern European order, the population is convinced that the move is justified and strengthens Russia's position in the region. After years of struggling to regain a vision and direction of post-Soviet Russia, the prime minister clearly has a distinct capability to guide and inspire the country.

Critical capabilities necessarily have critical requirements necessary for the COG to perform. Mr. Putin needs the support of the high-powered political class of Russia. Through many bold, aggressive government restructuring actions, he has created a block of politicians in the Federal Assembly and district governorships that solidify his overall support.[17] He also has earned and kept the support of the population at large. They believe that he is firmly in control, will act in the best interest of Russia, and is doing the right thing in exerting dominance over their sphere of influence. The backing of these two sectors is the key requirement to Putin's capability to lead Russia's spread of influence.

Finally, COG analyses determine the critical vulnerabilities based on the critical requirements. Any vulnerability would directly affect the support of both the political class and the greater population for Putin. If he was shown to be weak in the face of some sort of adversity, perhaps the support would waiver a bit, thereby weakening his will to continue pursuit of Russian regional hegemony. The political class, beholden to both legitimate and illegal businesses and traffickers, has already been weakened by the downturned economy. Further

action by another state against the Russian economy would threaten the "good life" they have, and if not immediately smashed by Mr. Putin, may lead to weakening of their support for him. This vulnerability could be exploited by a physical or information attack.

In addition, the greater population of Russia appears to support Mr. Putin out of a mix of pride and fear. Therefore, their support is vulnerable to emotional shifts. If the population perceives that Mr. Putin is unable to spread Russian influence abroad, protect Russia from incursion, or quell opposition among the masses at home, their support for his future actions could also wane. This vulnerability could be exploited by a military defeat on a battlefield, or an information campaign in the homeland.

---

[2] Blank, *Prospects for U.S.-Russia Security Cooperation*, 27-30
[3] Ibid., 30-32
[4] Ibid., 29
[5] E.U. Council *IIFFMCG Report*, 10
[6] Champion, "Tbilisi started '08 war"
[7] Joyner, "EU: Georgia 'Triggered' Illegal Invasion"
[8] Gomart, *EU-Russia Relations*, 3
[9] Blank, *Prospects for U.S.- Russia Security Cooperation*, 28
[10] Armstrong, 3
[11] Matthews, "Why Puppetmaster Putin is more dangerous than ever"
[12] Blank, *Prospects for U.S.- Russia Security Cooperation*, 28
[13] Tarlton, "Resurgent Russia in 2030," 5
[14] Matthews, "Why puppetmaster Putin is more dangerous than ever."
[15] Smith and Stewart, "It's Official: Putin finally admits…"
[16] Erlanger, "The World; Learning to Fear Putin's Gaze"
[17] Tarleton, "Resurgent Russia in 2030," 7

3. Deterrence Options

Deterrence can be defined as "the manipulation of an adversary's estimation of the cost/benefit calculation of taking a given action."[18] Deterrence of an adversary can be accomplished in two ways which can be used exclusively or in combination. The first is to increase the cost of the specific action above a certain threshold. The other is to lessen the benefit gained by the action—in effect lowering the threshold applied to the cost estimate. In other terminology, deterrence consists of two components: denial and punishment. Both components affect the cost-benefit calculation. Denial is the ability to frustrate attacks, thereby convincing the attacker that the action will not achieve their desired goals (lessens the benefit). Punishment is a threat of overwhelming retaliation that makes the cost of the action so great that it rises above the aforementioned threshold.[19]

Several keys to deterrence have been described by various theorists. General principles of deterrence include credibility, seriousness, capability, intentions and many others.[20] All theories seem to point to two critical factors; the willingness of the president to act, and the belief of other states in that willingness. The military and the Air Force in particular merely provide him with options. The decision on what option is best should be left up to the president and his security council. It is absolutely essential that after the president determines our deterrence strategy, he is able to convince all U.S. adversaries that our nation has the commitment and capability to implement his directions.

Scale of Deterrence

The U.S. president will make the best use of available response time if given a menu of discriminate preplanned response options from which to choose. This is the key to the flexible deterrent options (FDO) construct.[21] It is incumbent upon military planners and strategist to

provide options for the president. These options must cover a wide scale of response levels that can be matched to the level of belligerence of the adversary. In decades past, the options ranged from diplomatic pressure or economic sanction to air raids and on up to a full scale military invasion. The introduction of the atomic weapon further expanded the scale of FDO at the high end of the spectrum. Modern technology and reliance on computer networking has added another nuance to the FDO construct. Cyber-attack, or the threat thereof, has expanded the response scale somewhere in the middle. The RAND corporation published a modern concept of the scale of responses available to the president listing four levels of response pressure in order of belligerence: economic and diplomatic, cyber, physical force (conventional), and nuclear force.[22]

The lowest level of deterrence includes a range of diplomatic and economic actions. These include reduction of diplomatic ties, withdrawal of embassy personnel, or coordination of international support for friendly action and condemnation of an adversary's actions. Economic deterrence options are actions such as reduction in international aid, sanctions on imports or exports, or even seizing of real property that adversaries hold in the United States. Informational deterrence pressure is also a large part of economic and diplomatic deterrence. Any actions taken diplomatically or economically must be turned in to public support or condemnation both in the U.S. and internationally in order to have the fullest effect on the adversary.

RAND places pressure via threat of cyber-attack between diplomacy and physical force (non-nuclear). This is an extremely new concept in international relations. While many attacks have happened in the past decade, one case stands out as the first incident of cyber attack most likely attributed to a state actor meant to punish the action of another. In the spring of 2007, Russia allegedly executed weeks of internet attacks of distributed denial of service (DDOS)

attacks on its former satellite, Estonia, in response to their moving of an old Soviet war memorial. State web sites, banks and communication services were the targets. Estonia was particularly vulnerable to this sort of attack due to their web-based economy and 'paperless' government.[23] While the financial consequences of the attacks are not fully known, the societal disruption was clear.[24] In response to the activity, Estonia was forced to close off large portions of its network to users outside the country. Business people abroad could no longer access their bank accounts and government employees went without email for days.[25] This new form of pressure or threat bears further study as to its applicability to deterrence, especially since Russia now has first-hand experience with the damage it can inflict.

The highest levels of pressure the U.S. can use to deter an adversary both involve force and destruction. Conventional deterrence and posturing sends a clear signal to an actor considering some threatening move. A great example is the United States' actions during Operation Vigilant Warrior. On 6 October 1994, Saddam Hussein deployed two armored divisions southward to the Kuwaiti border. Within hours the United States rapidly began deployment of two Army mechanized brigades as well as a Marine Expeditionary force to deter Iraqi action against Kuwait. Additionally, the U.S. immediately dispatched aircraft carriers and Air Force assets to bolster the forces already in place. By 10 October, Hussein announced his intention to pull his divisions back.[26] It is perhaps the clearest case of conventional deterrence in recent history. It was also a major shift in deterrence theory of the U.S. military strategists. Until that time, deterrence was almost exclusively linked to nuclear weapons.[27]

Deterrence via threat of nuclear attack is the highest level of pressure available to a president. Nuclear deterrence theory is an entire field of study all on its own. After decades of competing viewpoints of how to best avoid a nuclear war between the U.S. and U.S.S.R., several

concepts emerged, including first-strike capability, survivability for second-strikes, and mutually assured destruction. Complete discussions of these theories are beyond the scope of this paper. For purposes of contemplating deterrence of Russia, one assumption holds. International opinion on nuclear strikes seems to be that they are only appropriate to respond to an in-kind attack.

U.S. Air Force Deterrence Options

Considering the four levels of deterrence described above, the Air Force has a capability to participate at three of them: cyber, conventional, and nuclear. U.S. military personnel may, on occasion, personally participate in diplomatic relations with foreign populations but not likely as part of coordinated and targeted deterrence. However, the other three levels have many areas where the Air Force and other services will participate. The Air Force is capable of performing cyber deterrence in many forms. They are currently sorting out their exact military role in cyberspace, but it will certainly be a major player, if not the leader in the Department of Defense. The Air Force has more clearly understood roles in deterrence via physical force with both conventional and nuclear weapon.

Since diplomatic and economic relations as well as nuclear deterrence theory are beyond the scope of this paper, the following two sections will analyze the global strike options of the U.S. Air Force to deter Russian aggression using cyber warfare, or prompt conventional strike. It bears repeating that the key to deterrence is the flexibility of options for the president. The options outlined below are the capabilities that the Air Force should develop to act as part of the deterrent strategy against Russia as described earlier. Analysis will reveal that each capability has advantages and drawbacks that the president must carefully consider.

[18] RAND *Six decades of deterrence*, 7
[19] Libicki, *Cyberdeterrence and Cyberwar*, 7 and Pape *Bombing to Win*, 18

[20] Herr, "Operation VIGILANT WARRIOR," Schelling, *Arms and Influence*, Libicki, *Cyberwar and Cyberdeterrence*, Pape, *Bombing to Win*.
[21] Joint Chiefs of Staff, *JP 5-0 Joint Operational Planning*, A-1
[22] Libicki, *Cyberdeterrence and cyberwar*, 29
[23] BBC News, "The cyber raiders hitting Estonia"
[24] Kramer, et al. *Cyberpower and National Security*, 525
[25] Landler, "Digital fears emerge after data surge in Estonia"
[26] Herr, "Operation VIGILANT WARRIOR," 25-26
[27] Ibid., 37

4. USAF Deterrence Capability: Cyber Global Strike

The concepts of cyber-war, cyber-attack, and cyber-deterrence are fairly new to national defense considerations. Most of the literature and doctrine is focused on protecting the United States' computer networks and infrastructure as well as deterring a cyber attack. On an UNCLASSIFIED level, the U.S. Air Force does have units that engage in offensive cyber-warfare[28], however, there appears to be a lack of strategic thinking about how these capabilities can be used as deterrence versus a way to gain a tactical advantage for a short term operation. Even if cyber threats are viable, one must consider whether or not offensive cyber attack is a smart strategy for the U.S. Air Force to pursue. The following section will examine the role that the Air Force could play in punishment of denial deterrence via threat of cyber attack and the advantages and disadvantages associated with that strategy.

Targets of Cyber Attack versus Russia

When choosing targets of cyber-attack, a basic understanding of the medium is required. Cyberspace and the associated target systems can be described as consisting of three layers, physical, syntactic, and semantic (or cognitive). All the information in cyberspace exists in a physical form in boxes, wires, and memory chips. Without this equipment, there is no longer a medium within which to operate. Above that level are the instructions, or software that tells the physical equipment how to operate. This is the syntactic level, which can also be removed or manipulated. At the highest level is the information itself in the form that users can understand; the reasons the system exists in the first place. The semantic level is where false or misleading information can in turn affect human beings and their behavior.[29] Cyber attacks against Russia could occur at any level, but based on the COG critical factor analysis presented earlier, they will be most effective at the syntactic and semantic level.

Russian strategists are aware of their cyber-vulnerabilities. Some policymakers feel that "the disintegration of the Soviet Union was due to a cognitive attack or deliberate information operation."[30] Consequently, Russian leaders are keenly focused on preventing a cyber attack focused on the emotional will of their populace (semantic level). The COG analysis showed that the emotional support of the populace is a requirement and vulnerability for Vladimir Putin. While Russia is no longer a closed, Soviet society, they are still conscious of information control to the masses. If the U.S. President wished to engage in a long-term cyber operation against Russia, he could choose to attack via the semantic level of cyberspace. The Air Force or other agency could engage in an information operation campaign via cyberspace to undermine the leadership's hold on the will of their population. The desired effect of this cyber global strike would be the weakening of their will to support military actions against their former satellites.

Unfortunately, the semantic cyber attack will not likely provide immediate deterrent effect. It is not clearly a direct threat in retaliation for a specific action. A more meaningful threat could be demonstrated at the syntactic level. As noted in the COG analysis, the Russian political elite are intertwined with their businesses, both legal and illegitimate. Cyber-warriors acting on orders of the president could prepare an attack on some important part of Russia's infrastructure. This course of action would demonstrate a coercive strategy via punishment, similar to our kinetic attacks against Serbia as part of operation Allied Force. During the air war over the ethnic cleansing of Albanian Muslims in Kosovo, the coalition forces struck Serb military units to the best of their ability. Even with consistent attacks on his ground forces, coalition strikes were unable to convince the Serb leader, Slobodan Milosevic, to end the cleansing by his troops. The top Air Force leader in Europe believed that the lack of capitulation was due to allied targeting of fielded forces instead of the Serb leadership. Once the air strikes

shifted emphasis to key economic infrastructure and industry, elite Serbs withdrew their support for Milosevic and he was force to end the ethnic cleansing. This is how syntactic cyber attack would work against Russia.

An effective syntactic cyber attack must hit the Russian elites just like the Serbs. The major economic resource for Russia is the oil and gas industry. As they rebuild and restructure their economy, the top businessmen will rely even more heavily on their vast deposits. The U.S. Air Force cyber warriors could target key nodes on the petroleum distribution system to cripple the industry and cut off they hard currency generator to the elite Russians closest to Vladimir Putin. More detailed estimation would likely involve classified discussion and is thus avoided in this paper. In short, the Air Force could offer an option to the president to target something of value to affect the will of Russia's elite populace in response to certain aggressive actions. If Mr. Putin is unable to stop it, such an attack could weaken support for him, the strategic COG. This would be the most effective threat of cyber-attack resulting in strategic deterrence, especially considering the damage from both Allied Force and the Estonia cyber-attack witnessed first-hand by Russia.

Advantages of Cyber Global Strike

The asymmetric advantages of cyber attack are well documented.[31] An attack may come from a single malicious entity using one machine to directly affect another, larger system. The attacker can multiply his efforts by co-opting dozens or hundreds of other machines without their owner's knowledge. Clearly, the cost of such an endeavor is completely out of proportion to the damage it could cause to a target system. The U.S. Air Force can exploit this asymmetry when considering cyber-threat as a means of deterrence against other states. A small, dedicated cadre of highly trained cyber-warriors within the USAF can, in some cases, inflict as much damage on

a target state as several wings of attack aircraft. Even better, they can do it from their home station without aerial refueling, suppression of enemy air defense, and other supporting assets required by a package of attack aircraft. Of course, as with airpower, the effectiveness of cyber attack depends greatly on many contextual factors such as target vulnerability and their reliance on technology and interconnectivity.

The asymmetry of cyber-attack is enhanced further by the immense costs to defend against it. Powerful organizations like the Air Force have already spent countless dollars in technology and man-hours to defend against this threat. This is evidenced by the scores of research papers, books, and volumes of doctrine and computer network tactics, techniques and procedures published regarding cyber defense. Developed nations that are increasingly dependent on cyberspace will continue to spend billions in this effort. Additionally, in a similar conundrum as anti-terrorism strategies, the defending nation has to protect itself all the time, whereas a cyber attacker sometimes has to be successful only once to create the desired effect.

A second major advantage of cyber-attack is the lack of bloodshed that results directly. Certainly, a large-scale cyber-attack could cripple a state's economy, possibly resulting in some injuries or death. But generally, the lack of direct attribution of human deaths to the attacker may offer some advantage to a nation wishing to threaten cyber-attack as part of a deterrence strategy. Regarding the deterrence of Russian aggression, it will be extremely difficult to convince Mr. Putin that the U.S. will attack his troops with bombers and cruise missiles over a former satellite's sovereignty. After decades of the Cold War and dozens of confrontations with the Soviets, it seems clear that the U.S. leadership will do almost anything to avoid a direct military clash with Russia. However, if the Air Force can threaten to shut down Russian hydro-electric plants, gas pipelines, or their entire banking system via a covert cyber-attack that won't

directly harm any citizen or soldier, it is more likely that the Russian leadership can be convinced of our willingness to act.

Finally, the U.S. must consider international reaction to any deterrence strategy. In recent decades, the United States has been repeatedly accused of premature use of military force, or "reaching for the gun" in international affairs. As stated above, the key to deterrence and national strategy is to offer many different options to the president. The threat of cyber-attack allows the President another level of pressure that does not quite reach the realm of physical force. From an international perspective, if the U.S. were to threaten to execute a cyber-attack versus a kinetic strike perhaps the U.S. would not seem so prone to violence as is often purported. As demonstrated by the United States' involvement in Iraq since 2003, international opinion on our actions has far-reaching effects on relations with other countries even in matters unrelated to the military.

Disadvantages of Cyber Global Strike

Any deterrence strategy will have weaknesses. Cyber attack is no different, however, the disadvantages are not as obvious or intuitive. The first major disadvantage exists in the threat itself. Any state or actor threatening a cyber attack will necessarily indicate the nature of the attack, thereby allowing the target an opportunity to defend itself. The threatening actor must consider carefully how much to reveal when making the threat so as to divulge enough detail to demonstrate resolve and seriousness, but not so much as to present an opportunity for the target to develop an effective defense. This conundrum doesn't exist the same way in conventional warfare. A threat of physical force can be made more generically. Even if specific details are provided, a stronger attacker will still succeed. The world of cyberspace is different. There is

not currently a capability so strong as to render any defense powerless. Even in the worst circumstances, a target can always disconnect itself from the global information grid.

In a similar way, a cyber attack is not repeatable in the same manner as a physical strike. An actor executing a punishment deterrence strategy using kinetic action versus an aggressor can keep striking back until the desire effect has been achieved or his attacks are physically repulsed. However, once a cyber attack occurs the details as to how it worked are usually readily apparent to the target. Consequently, the target can quickly develop a defense against that attack negating the opportunity for repetition. Hence no further harm can come from a similar attack and the deterrent effect is lost. The attacker must develop another strike using dissimilar methods to regain the advantage. To summarize, cyber attacks usually result in the strengthening of a target's defenses.

Cyber Global Strike Conclusions

The option of cyber attack to deter Russian aggression is just that; an option. The president has to account for many factors when making the decision to use this method of deterrence. It is critical to develop the capability to apply pressure via threat of cyber-attack and to tailor that capability to best affect the strategic COG, Mr. Putin. The threat should be a short term, repeatable action. This means that the Air Force should focus cyber attack efforts on the petroleum distribution system or other business assets most important to the political class of Russia. This would have the greatest impact on their support for Mr. Putin and be a measureable, clear threat in response to specific action by the Russians. The elites must suffer some damage and they must believe he was unable to counter the attack. They also must be convinced that their situation will not improve unless the Russian leadership discontinues the action that brought on the cyber global strike. The U.S. must be prepared to let the initial attack

sink in, and repeat the action as necessary, with modifications if required, until the desired response is achieved.

The U.S. must also be ready for a possible unintended consequence of a cyber attack in response to a Russian action against their former Soviet partner nations. The attack may actually increase the resolve of Russia to see their aggression through to fruition. This effect is best summed up by Martin Libicki in *Cyberdeterrence and Cyberwar*:

> "A cyberwar that hits home might have a greater influence on the relationships between two powers than a battlefield war would, despite the casualties the latter would cause. Yet attacking the homeland, even if only in cyberspace, might elevate the importance of achieving military goals in faraway lands because the contest may be viewed as correspondingly strategic."[32]

In other words, by exerting deterrence pressure via cyber attack, Libicki warns the U.S. may drive Russia to feel their success on the battlefield becomes a strategic issue rather than a localized matter. The increased importance they might place on the small conflict may unfortunately backfire and increase Russian resolve. Consequently, U.S. leaders must consider that a cyber attack on the population of Russia is an inherently strategic act with strategic consequences.

[28] 24th Air Force Factsheet
[29] Libicki, *Cyberdeterrence and Cyberwar*, 12
[30] Kramer et al. *Cyberpower and National Security*, 477
[31] Libick, *Cyberdeterrence and Cyberwar*, 122
[32] Ibid., 124-125

5. USAF Deterrence Capability; Non-Nuclear Kinetic Global Strike

The Air Force has a much more traditional role in deterring Russian regional aggression. In addition to supporting a conventional force buildup in the region, the Air Force has an unmatched capability to employ physical force within hours or days, halfway around the world, using a variety of current and planned weapons systems. These weapons would be used in both denial and punishment deterrent strategies. When used for denial, traditional attack aircraft can fortify the defense of a weaker state by halting attacking Russian forces long enough to allow follow-on forces. The effectiveness of an air-only campaign to halt a fielded army has been debated heavily with air power advocates successfully arguing in many circles that it can be accomplished.[33] Attack platforms have a much clearer role, however, when used as part of a punishment strategy. Long range bombers and missiles can be used to threaten credible, physical harm to targets valued by Russia both within their borders and in surrounding states in response to aggressive action. The following chapter examines several ways the Air Force can employ conventional, kinetic global strike at the present time and in the near future.

Intercontinental Bombers: Long-Range Standoff Weapons and LO Direct Attack

The Air Force's three bombers represent the core of global strike capability. With adequate aerial refueling support, the B-1, B-2, and B-52 can launch from bases in the continental United States (CONUS) and fly anywhere in the world non-stop in less than 24 hours. Upon arrival aircrew can then deliver significant numbers of precision weapons that may affect dozens of targets with a single formation of aircraft. However, this would require either a permissive environment or a large support package that would have to be based much nearer to the battlespace; likely reducing the promptness of the attack. Alternatively, all three aircraft are configured to launch long-range, standoff missiles capable of hitting—with near-precision—

targets hundreds of miles away without endangering the bomber or crew. With these weapon systems, the Air Force presents the president with the option to pressure Russia via threat of physical attack as part of a denial or punishment deterrent strategy.

The B-52 has long since been modified to carry cruise missiles, both nuclear and conventional. Presently, up to 20 AGM-86 Conventional Air-Launched Cruise Missiles (CALCMs) can be carried by a single aircraft.[34] These weapons have been used successfully in operations Desert Storm, Desert Fox, Desert Strike, Allied Force, Enduring Freedom and Iraqi Freedom. All of the bombers, including the B-1 and B-2 have been recently modified to launch the AGM-158 Joint Air to Surface Standoff Missile (JASSM). The B-1 carries 24 JASSM, the B-2, 16, and the B-52, 12. The JASSM is a low-observable (LO) weapon that can strike targets using a 1,000 pound warhead and millimeter wave, precision terminal area seeker. It is approximately half the cost of the AGM-86 and much simpler to employ. While not a true cruise missile in terms of flight profile and range, the extended range version can reach over 400 nautical miles and promises to be very survivable, even against modern air defenses.[35]

In addition to launching JASSM from outside Russian airspace, the B-2 provides the president with an option to covertly strike targets either inside Russia or within air defense coverage of their forces in neighboring countries. The LO capabilities of the B-2 means that it can put near-precision weapons like Joint Direct Attack Munition (JDAM) directly on targets in greater numbers than if using only JASSM. In fact, one B-2 can place 80 500-pound JDAM on target in a single pass versus just 16 JASSM. Exploiting LO technology, the B-2 could penetrate hostile airspace and launch a much more decisive halting attack versus Russian formations and egress the threat area before air defenses could be activated. This provides the president with another more devastating option, if desired, to pressure Russia to reconsider aggression.

As noted above, the bombers can be used effectively in both denial and punishment deterrent strategies. To create deterrence via denial, the defender must convince the attacker that his action has little hope of success in relation to the cost required. Traditionally, denial would be achieved by massive, rapid, conventional buildup as in Operation Vigilant Warrior.[36] However, planners should also consider the use of global strike assets in this situation. If ordered, formations of intercontinental bombers carrying JASSM or CALCM could be used to attack semi-fixed or permanent Russian military forces in an effort to stop their assault on a neighboring state. Additionally, given a more permissive environment, the bombers could halt the invasion forces with large numbers of JDAM or anti-armor cluster munitions such as CBU-103, 104, and 105. The bombers could fly from bases in the continental United States, negating the requirement of forward basing. They would, however, require massive amounts of refueling support from tankers already scattered around the globe.

It is much easier to envision the bombers used in a punishment strategy. Those familiar with nuclear deterrence during the Cold War will recall the massive retaliation strategy pursued by the Eisenhower administration. The administration's theory was that the Soviet Union could be deterred from military aggression by the assurance of a massive retaliatory nuclear strike by U.S. bombers in response to such action. This concept can be adjusted slightly to be applied to the current strategy vis-à-vis Russia. While not delivering a massive nuclear attack, Air Force bombers could fly around the world and conventionally strike targets of value to the Russian leadership as a punishment in response to aggression. Any of the bombers are capable of launching JASSM and CALCM on pre-planned, high value targets in response to Russian aggression. As noted above, B-2s could also penetrate Russian airspace to deliver a heavier load of JDAM. This would be a reaction *after* the aggressive act. In order to serve as a deterrent

against that action, it would be incumbent on our president to convince Mr. Putin that we are willing and capable of such a strike if *they* chose aggression. That is the most difficult part of this strategy. The Air Force can aid the president's efforts by maintaining a legitimate, competent, and powerful global strike force that can perform as promised.

Advantages & Disadvantages of Bomber Deterrence

When determining whether or not to use the bomber force, the president must consider the inherent advantages and disadvantages. There are many positive aspects of the intercontinental bomber as a conventional deterrence tool. First of all, they can offer the president a quick reaction with less commitment. When used in the global strike role, the bombers can launch and recover from bases in the CONUS. This allows action against Russian aggression without waiting for a large force buildup. Assuming tanker assets are available across the Atlantic and Europe, our bomber force could have weapons on target in 24 hours or less. This quick, global strike strategy also avoids difficulties with basing rights and international overreaction. While the buildup of troops as part of Vigilant Warrior to defend Kuwait against another Iraqi invasion in 1994 was palatable to the international community, the same is not likely true if American troops massed in support of a former Soviet satellite against Russian aggression. Launching and recovering from the CONUS avoids all that discontent.

Ironically, the president could also use the bomber force in the exact opposite way to achieve his desired effect. As noted above, a key tenet of deterrence is to convince the aggressor of your resolve or "seriousness." One way to demonstrate that is through deployment of forces closer to the aggressor. All three of the bombers have been successfully forward deployed to locations all around the world. Rather than avoiding international reaction by launching from home airfields, the president can instead send a message via the Air Force by deploying any of

the bombers to forward operating locations (FOLs) within easy reach of Russian territory without requiring aerial refueling. The message to Russia and the world would be that America is serious and committed to defend the sovereignty of any nation against their re-exertion of regional hegemony.

Disadvantages of employing our bomber forces are also numerous. When analyzing a conflict with Russia, one immediately should realize that Russia has thousands of nuclear weapons capable of striking the United States. The president must ensure that any U.S. kinetic action first and foremost does not trigger Russian nuclear counteraction. The most critical way to avoid catastrophe is to not indicate to the Russians that American hardware is trespassing on their sovereign territory. In other words, if bombers are employed as described above it is critical that they are not observed penetrating Russian airspace. If they are directed to attack targets inside Russia either to halt attacks as part of denial or eliminate targets as a punishment strategy, they must use LO technology in the form of the B-2 or JASSM. It does not negate the fact that our hardware is over Russian territory, but perhaps it could create some plausible deniability long enough to stifle any thoughts of nuclear retaliation.

There are some other limitations of the bomber force when used to halt an invasion that planners must consider. The long flight time of CALCM and JASSM (tens of minutes) renders them useless against any target that may move within that time. The B-1 does have a capability to launch a pattern of JASSM on a moving target tracked by its radar, but the cost of such attack (in terms of payload consumption) due to the number of required weapons would likely be prohibitive. Secondly, due to the long standoff ranges of the JASSM and positive identification limitations when employing JDAM, the bombers need target data from some off-board source. This would have to be near real-time information. Ideally, it would come from an element on the

ground which would require deployment of qualified joint terminal air controllers (JTACs). More likely, targeting data would come from an airborne reconnaissance platform, like the MQ-1, MQ-9, or future remotely piloted aircraft (RPA). The details of deploying these assets to the area of operations would, of course, be a critical consideration of the planning process; one that may seriously limit the bomber's effectiveness.

One final disadvantage is the escalation that it would signal to the rest of the world. As discussed above, unintended effects are often created by actions that send messages to the entire world. The message indicated by any American kinetic actions against Russia will be resounding, especially actions by nuclear-capable bombers. After more than a half century of a Cold War where the world was on the brink of nuclear disaster, the prospect of American weapons killing Russian troops could trigger visions of the apocalypse among the nations of the world. The same message could result simply from having American bombers penetrate Russian airspace. Any president considering kinetic deterrence actions must heavily weigh the message that would be passed to Russia and the rest of the world.

Future U.S. Air Force Conventional Global Strike Options

The U.S. Air Force is constantly reevaluating the future of long range strike. Currently, there is great debate as to whether the next platform will be manned or unmanned, traditional jet powered or some sort of hypersonic, near-space vehicle. In any case, the capabilities it will bring will be similar to our current force and can be applied to Russian deterrence in similar ways. There is, however, another global strike capability that is possible in the near future and warrants analysis. For many years, the concept of "prompt global strike" has been under development. In 2004 the Defense Science Board (DSB) studied different ideas for prompt response weapons and included the concept of conventionally armed ICBMs.[37] With the

drawdown of the U.S. Air Force's nuclear ICBM force, there are dozens if not hundreds of missiles available to be converted to conventional use. The adaptive technology is fairly mature and could be fielded within three years if provided the funding and given an aggressive development schedule.[38] The Air Force could conceivably finalize the employment of these weapons to provide yet another deterrent option against Russian aggression.

Conventional global strike capability deployed on ICBMs provides many critical components of deterrence. Like conventional attacks from long range bombers it can be used as part of denial or punishment strategy with the same advantages and drawbacks. However, it would immensely improve the rapidity of response to Russian actions. Also, it would require no tanker support, and only limited targeting assets deployed to support strikes. Finally, while initially expensive to convert the missiles, follow-on support and employment costs would make them actually cheaper in the long run than manned long-range bombers.

However, there is one major drawback that may virtually eliminate the conventional ICBM as a tool in the deterrence of Russia. As described above, the worst outcome of any deterrence via conventional strike on Russia would be a nuclear retaliation from them. A phrase "nuclear ambiguity" has been coined to describe the uncertainty that arises when an ICBM is launched. It is described below by the National Research Council's committee on conventional prompt global strike.

> If another country, for example Russia or China, were to detect the launch of one or more conventionally armed long-range missiles from a deployed SSBN [or ICMB], how might it interpret the event? There are two aspects, logically and practically distinct, of the nuclear ambiguity issue. The first is the possible misinterpretation by an observing nation of a conventional strike on a third party as a nuclear strike on its own territory. The second is the possible misinterpretation by an observing nation of one or more conventionally armed missiles headed toward its territory as a nuclear attack. The ambiguity issue is more significant in the second case.[39]

As described by the committee, Russia may be tempted to respond when ICBMs are streaking towards their territory, conventional or not. This is exactly what could occur if the United States were to use conventional ICBMs in a deterrence situation.

There are, however, ways to mitigate the dangers of nuclear ambiguity. The Air Force would have to develop an impenetrable firewall between nuclear and conventional ICBMs, demonstrating very clearly to the rest of the world that specific missiles are purely conventional. Another recommendation is to field conventional ICBMs only on the coast. In that manner, other nations with surveillance capabilities could observe a launch from one of America's shorelines and be assured that it is a conventional warhead. Similarly, the trajectory of the weapons could have certain characteristics that would mark it as conventional. Additionally, coastal basing eliminates the problem of spent missile boosters falling back to earth in populated areas. Obviously, this was never a concern when planning for nuclear ICBM basing due to their launches occurring only in the direst of circumstances. If the missiles are converted to conventional warheads, they are more likely to actually be used.

The key to all of these mitigation techniques is transparency. Rival nations must have a degree of insight in to our doctrine and operations to be reassured that they can trust our intentions. Unfortunately, if deterrence of Russia has progressed to the point of conventional ICBM strike, all trust may already be lost. It seems that the concept of conventional ICBMs may have too many complications to serve as a realistic and effective deterrent tool. The Navy is undertaking a more practical conversion by swapping out nuclear-armed, submarine launched ballistic missiles (SLBMs) with conventional cruise missiles on some of its Ohio-class submarines.[40] Launching conventional cruise missiles or short-ranged SLBMs from these ships

will eliminate many of the complications discussed above faced by Air Force conventional ICBMs. In light of these challenges, this capability is best left to the Navy to develop.

[33] Haun, "Airpower versus a Fielded Army," 2 Summarizes several Air Power arguments
[34] *Long Range Strike*, U.S. Air Force whitepaper, D-1
[35] Lockheed Martin. AGM-158 JASSM Product Card
[36] Herr, "Operation VIGILANT WARRIOR"
[37] Hebert, "The ICBM Makeover"
[38] Lichterman, "Space Planes…," 2. Quoting an excerpt from the U.S. Air Force Space Force Application Mission Area Development plan, 1995, p 35.
[39] Committee on CBGSC, "Prompt Global Strike," 11
[40] "SSGN Tactical Tridents"

6. Conclusion

It appears Russia has no intention of backing off the desire to be the regional hegemon in the former "near abroad" sphere of former Soviet territories. For the United States or the European Union to challenge that dominance is a delicate task. The pressure that Russia exerts on its neighbors will likely be similar to the action against Georgia in 2008. Aggression will be largely behind the scenes and any overt moves will be justified in terms of self-determination of oppressed ethnic Russians. In that context, it will be difficult to muster international regimes to counter them. Additionally, their military actions will likely be very incremental and just below any threshold that would garner support for military response.

In light of this, the U.S. president will rely heavily on diplomacy and economic actions when dealing with the Russians. Since the Russians seem to be limiting their influence to their immediate neighbors in Europe and Asia, it is critical that American leaders are mindful of international opinion and seek agreement from other regional players before taking any action. When pursuing deterrence, the U.S. leaders should lead with international efforts at diplomacy first, but make it clear that they are willing to employ military force or hostile information warfare to shape Russian behavior.

If military action is required as part of deterrence, the U.S. Air Force will have critical capabilities to offer the president. Besides the obvious and well established nuclear deterrence mission, the Air Force can offer less drastic options. First, the Air Force should continue to develop a large contingent of "Cyber-Warriors" trained to execute carefully focused cyber attacks on petroleum distribution system targets considered most vital to the Russian political class. The same war-fighters should be teamed with information warfare experts to prepare cyber attack at the cognitive level to affect the opinion and motivation of the greater Russian population that support their aggression. Fortunately, in recent years Air Force leadership has

recognized this need. The 67th Network Warfare Wing has received large increases in the number of positions for network warriors and has become the largest operational wing in the Air Force. It will take still more years to fully integrate and train their new accessions, but the process has at least begun.[41] Further development of this capability is a major aspect to future flexible deterrent options and is provides the widest range of effects within the deterrence spectrum.

Kinetic action is also still a major part of deterrence. World leaders of course desire never to actually carry out the threats made as part of negotiations, but the threat must be credible. To maintain that credibility, the best non-nuclear global strike capability that the U.S. Air Force can provide in future deterrence of Russia is the combination of intercontinental bombers and cruise missiles, specifically the AGM-158 JASSM. The cost, range, accuracy a LO qualities of the JASSM all contribute to its effectiveness as a credible deterrent tool. The global ranges of the three bombers allow them to launch from CONUS and strike Russian targets in or near any of the former Soviet republics in roughly 24 hours. In my opinion, the Air Force needs to continue the production and implementation of the JASSM in the extended range variant (JASSM-ER). Additionally, the Air Force should maintain the fleet of long-range, heavy bombers as it stands. Smaller aircraft like the F-16 and F-35 will be able to employ the JASSM-ER as well, but do provide the prompt global strike capability inherent in the bomber force.

Through development of these two capabilities, the Air Force can provide options for prompt global strike to the president. As emphasized several times, the key to flexible deterrence is a variety of options. With viable cyber and conventional global strike capabilities, the United States has a more complete array of options available from diplomatic actions all the

way to nuclear retaliation. How the president decides to leverage these options is the true key to national security and power.

[41] "Cyberspace Power," Air Command and Staff College Lecture, AY10

Bibliography

Adee, Sally. "The Hunt for the Kill Switch." *Spectrum*, May 2008. http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch (accessed 9 December 2009).

Air Force Space Command Public Affairs. *24th Air Force Factsheet*. Peterson AFB, Colorado: October 2009.

Armstrong, Bradley J., Maj USAF. "Confronting Russia, Again." Research Report, Air Command and Staff College, 2009.

Blank, Steven J., ed. *Prospects for US Russia Security Cooperation.* Carlisle, PA: The Strategic Studies Institute, 2009.

Blank, Steven J., ed. *Towards a New Russian Policy.* Carlisle, PA: The Strategic Studies Institute, 2008.

Campbell, Matthew. "'Logic Bomb' Arms Race Panics Russians." *The Sunday Times*, 29 November 1998. http://cryptome.org/jya/ru-panic.htm (accessed 9 December 2009).

Champion, Marc. "Tbilisi started '08 war, but Moscow also at fault, EU finds." *The Wall Street Journal.* 1 October 2009. http://online.wsj.com/article/SB125431087432152321.html (accessed 13 February 2010).

Council of the European Union. *Independent International Fact-Finding Mission on the Conflict in Georgia*. http://www.ceiig.ch/Report.html (accessed 13 February 2010).

Cullison, Alan, and Yochi Dreazen. "Moscow Moves to Counter U.S. Power in Central Asia." *The Wall Street Journal*, 5 February 2009. http://proquest.umi.com/pqdweb?did=1638553701&sid=1&Fmt=3&clientId=417&RQT=309&VName=PQD&cfc=1 (accessed 11 Dec 2009).

Erlanger, Steven. "The World; Learning to Fear Putin's Gaze." *The New York Times.* 25 February 2001. http://www.nytimes.com/2001/02/25/weekinreview/the-world-learning-to-fear-putin-s-gaze.html (accessed 24 February 2010).

Espiner, Tom. "US Reveals Plan to Hit Back at Cyber Threats." *ZDNet News*, 2 April 2008. http://news.zdnet.co.uk/security/0,1000000189,39378374,00.htm (accessed 9 December 2009).

"Estonia Fines Man for 'Cyber War." *BBC News*. 25 January 2008. http://news.bbc.co.uk/2/hi/technology/7208511.stm (accessed 9 December 2009).

"Estonia hit by Moscow Cyber-War." BBC News. 17 May 2007. http://news.bbc.co.uk/2/hi/europe/6665145.stm (accessed 13 February 2010).

Ibid. "Georgia Accuses Russia of Coordinated Cyberattack." *CNET News*, 11 Aug 2008. http://news.cnet.com/8301-1009_3-10014150-83.html (accessed 9 December 2009).

Joyner, James. "EU: Georgia 'Triggered' Russia's Illegal Invasion." *New Atlanticist*. 30 September 2009. http://www.acus.org/new_atlanticist/eu-georgia-triggered-russias-illegal-invasion. (accessed 13 February 2010).

Gale, David A., Maj USAF. "Cyber-MAD: Should the U.S. Adopt a Mutually Assured Destruction Policy for Cyberspace?" Research Report, Air Command and Staff College, 2009.

Gomart, Thomas. *EU-Russian Relations: Toward a way out of Depression*. Washington D.C.: Center for Strategic and International Studies, 2008.

Gorman, Siobhan. "Georgia States Computers Hit by Cyberattack." *The Wall Street Journal*, 12 Aug 2008. http://online.wsj.com/article/SB121850756472932159.html (accessed 9 December 2009).

Hart, Kim. "Longtime Battle Lines are Recast in Russia and Georgia's Cyberwar." *Washington Post*, 14 August 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html (accessed 9 December 2009).

Haun, Phil M. "Airpower versus a Fielded Army: A Construct for Air Operations in the 21st Century." Research Report, Air Command and Staff College. 2001

Hebert, Adam J. "The ICBM Makeover." *Air Force Magazine*, October 2005. http://www.afa.org/oct2005/1005ICBM.html (accessed 28 February 2010).

Herr, Eric W., Maj USAF. "Operation Vigilant Warrior: Conventional Deterrence Theory, Doctrine, and Practice." Thesis, School of Advanced Air and Space Studies, 1996.

Kramer, Franklin D. et al eds. *Cyberpower and National Security*. Dulles, VA: National Defense University Press and Potomac Books, 2009.

Landler, Mark, and John Markoff. "Digital fears emerge after data siege in Estonia." The New York Times. 29 May 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=2&_r=1 (accessed 13 February 2010).

Libicki, Martin C. Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND Corporation Project Air Force, 2009.

Lichterman, Andrew M. "The Military Space Plane, Conventional ICBMs and the Common Aero Vehicle: Overlooked Threats of Weapons Delivered Through or from Space." *Western States Legal Foundation Information Bulletin*. Fall 2002.

Lockheed Martin. *JASSM Weapon Product Card*. Dallas, Texas: 2008. http://www.lockheedmartin.com/data/assets/mfc/PC/MFC_JASSM_PC.pdf (accessed 1 April 2010).

London, Jack R. Jr, Lt Col, USAF. "The Ultimate Standoff Weapon." *Air Power Journal*. Summer 1993.

Long, Andrew. *Deterrence: From Cold War to Long War*. RAND Monograph. Santa Monica, CA: RAND Corporation, 2008.

Long Range Strike. US Air Force White Paper. Washington, DC: HQ USAF/A5RC, 2007.

Matthews, Owen. "Why puppetmaster Putin is more dangerous than ever." *London Daily Mail*. 12 August 2008. http://www.dailymail.co.uk/news/article-1043684/Why-puppetmaster-Putin-dangerous-ever.html (accessed 18 February 2010).

McDermott, Roger. "Russia's Air Force Modernizes for a 'Virtual Cold War.'" *Eurasia Daily Monitor*, Vol 6, Issue 31, 17 February 2009. http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=34513 (accessed 11 Dec 2009).

National Research Council Committee on Prompt Global Strike Capability. *U.S. Conventional Prompt Global Strike: Issues for 2008 and beyond.* Washington DC: National Academies Press 2008.

Office of the Deputy Assistant to the Secretary of Defense for Nuclear Matters. "US Nuclear Deterrence – Nuclear Stockpiles." http://www.acq.osd.mil/ncbdp/nm/USNuclearDeterrence.html (accessed 11 December 2009).

Owens, Christopher G., COL US Army. "The Promise and Peril of the New Strategic Triad." Strategic Research Project, U.S. Army War College, 2003.

Oznobishchev, Sergey. "Prospects for US-Russian Arms Control and Disarmament: A Russian Perspective." Strategic Insights, Vol VIII, Issue 4 (September 2009).

Pape, Robert A. *Bombing to Win*. Ithaca, NY: Cornell University Press, 1996.

Rutland, Peter. "The Reset Misfires." *The Moscow Times*. 12 February 2010. http://www.themoscowtimes.com/opinion/article/the-reset-misfires/399596.html (accessed 18 February 2010).

Schelling, Thomas C. *Arms and Influence.* New Haven, CT: Yale University Press, 2008.

Smith, Graham, and Will Stewart. "It's Official" Putin finally admits nouveau riche Russians really DO have bad taste and show off all the time." *London Daily Mail*. 3 December 2009. http://www.dailymail.co.uk/news/worldnews/article-1233002/Its-official-Putin-finally-admits-nouveau-riche-Russians-really-DO-bad-taste-time.html (accessed 18 February 2010).

"SSGN "Tactical Trident" Subs: Special Forces and Super Strike." *Defense Industry Daily*. 28 September 2009. http://www.defenseindustrydaily.com/ssgn-tactical-trident-subs-special-forces-and-super-strike-01764/#readings (accessed 3 March 2010).

Tarleton, Michael F., Lt Col USAF. "Resurgent Russia in 2030: A Study of the Past, Present, and Possible Future Political Situation with the Russian Federation." Research Report, Air War College, 2008.

"The Cyber-Raiders hitting Estonia." *BBC News.* 17 May 2007. http://news.bbc.co.uk/2/hi/europe/6665195.stm (accessed 13 February 2010).

Uemura, Robert K., Lt. Col USAF. "Formula for Deterrence: The Challenge to Deterring Contemporary Threats to U.S. National Interests." Research Report, Air War College, 2008.

Vandiver, Samuel B., Maj USAF. "Russia's Great Power Security Relationship with the United States." Research Report, Air Command and Staff College, 2003.